عرض مشاركة واحدة

**الموضوع**: الآن ..شرح كيفية عمل التور ...و كيف يمكن لأجهزة الأمن و المخابرات إصطيادك كالسمكة ...!!

14-08-2010 #**1**

مُلاعب الأسنة
شامخ مميز

المشاركات : 2,716

**الآن ..شرح كيفية عمل التور ...و كيف يمكن لأجهزة الأمن و المخابرات إصطيادك كالسمكة ...!!**

# الآن ..شرح كيفية عمل التور ...
# و كيف يمكن لأجهزة الأمن و المخابرات
# إصطيادك كالسمكة ...!!

**ملاحظة1**

**المرجو من الإخوة المشرفين ترك الموضوع هنا لأن أمن الإخوة يمر قبل كل شئ**

**ملاحظة2**

**هذا الموضوع لا يشرح كيفية تنصيب التورTOR لأنه تم شرح التنصيب في قسم الكمبيوتر**
**و تم الإجابة على جميع المشاكل التي واجهت الإخوة خلال عملية التنصيب و يمكنك**
**مراجعة الشرح + الردود ( التي هي أهم من الشرح لأن فيها حلول المشاكل )**

**http://202.75.39.82/~alfaloj/vb/showthread.php?t=31643**



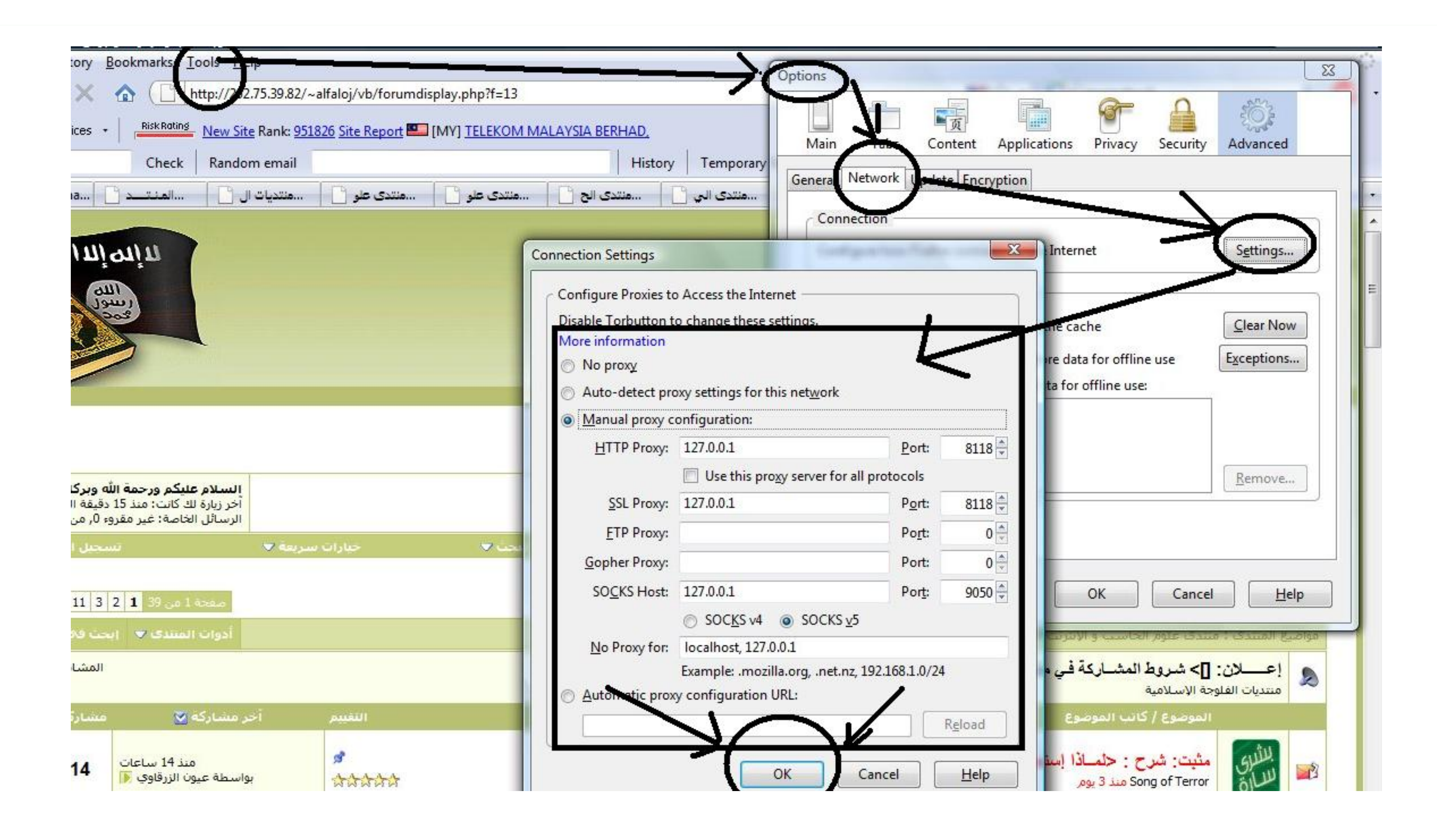
**سنقـــوم في هذا الموضوع بشرح كيفية التخفي و سد ثغرات خطيرة جدا و أنصح بقراءة الموضوع بتركيز شديد فلربمـــا يكون هذا الموضوع سببا في إفشال عملية إصطيادك من طرف أجهزة الأمن و المخابرات في البلد الذي تقطنه و اختفائك من المنتدى كمـــا اختفـــى المئـــات من قبلك ...**
**و لا تنسى أن أدعية الصباح و المساء هي من أسباب تماما كما أن استعمال وسائل التخفي من الأسباب و الله أمرك بالأخذ بجميـــع الأسباب ...**

**هنـــاك أمرين مختلفين تمـــامـا و هما :**
**1**
**برنامج التور**
**2**
**المتصفح ( firefox أو opera أو IE أو... أو .... ) الذي ستتعمله**

**نقوم بالتخفي من خلال أمر المتصفح الذي نستعمله بتمرير إتصاله عن طريق التور و ذلك يكون :**

**بتعديل بيانات المتصفح ليقوم متصفحك ( firefox أو opera أو IE أو... أو .... ) بـتمرير إتصاله عن طريق التور و هذا مثال لذلك :**

.This image has been resized. Click this bar to view the full image. The original image is sized 1156x657




اقتباس:

إذا دققـت في الصورة جيدا تكتشف أنك تأمر متصفحك بتمرير البيانات من جهازك إلى جهازك مرة أخرى!!! ( Localhost أي 127.0.0.1) عن طريق البورت رقم 8118 لأن جهازك مركب عليه سرفر صغير إسمه PRIVOXY و PRIVOXY هـذا هو الذي يقوم بإعادة تمرير البيانات إلى العالم الخارجي ( أو ما يسمى بالإنترنت ) عن طريق استعمال البورت رقم 9050

ملاحظة

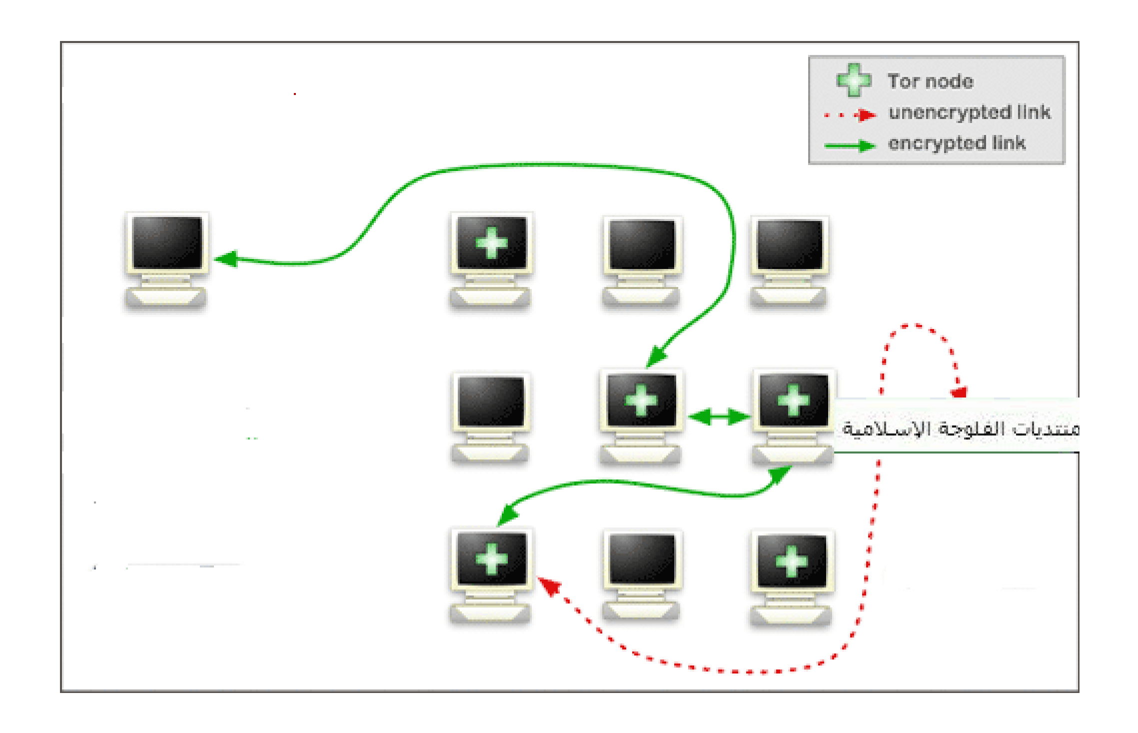
إذا كنت تستعمل متصفح FireFox فيمكنك تجاوز هذه الخطوة من خلال استعمال أداة Torbutton التي تقوم أوتوماتكيا بهذه العملية عند الضغط عليها

**اذن الباكيت تخرج من متصفحك بواسطة بروتوكول الhttp من المنفذ 8118**

**لتذهب إلى ( localhost 127.0.0.1) سرفر ال*Privoxy* المركب على جهازك**

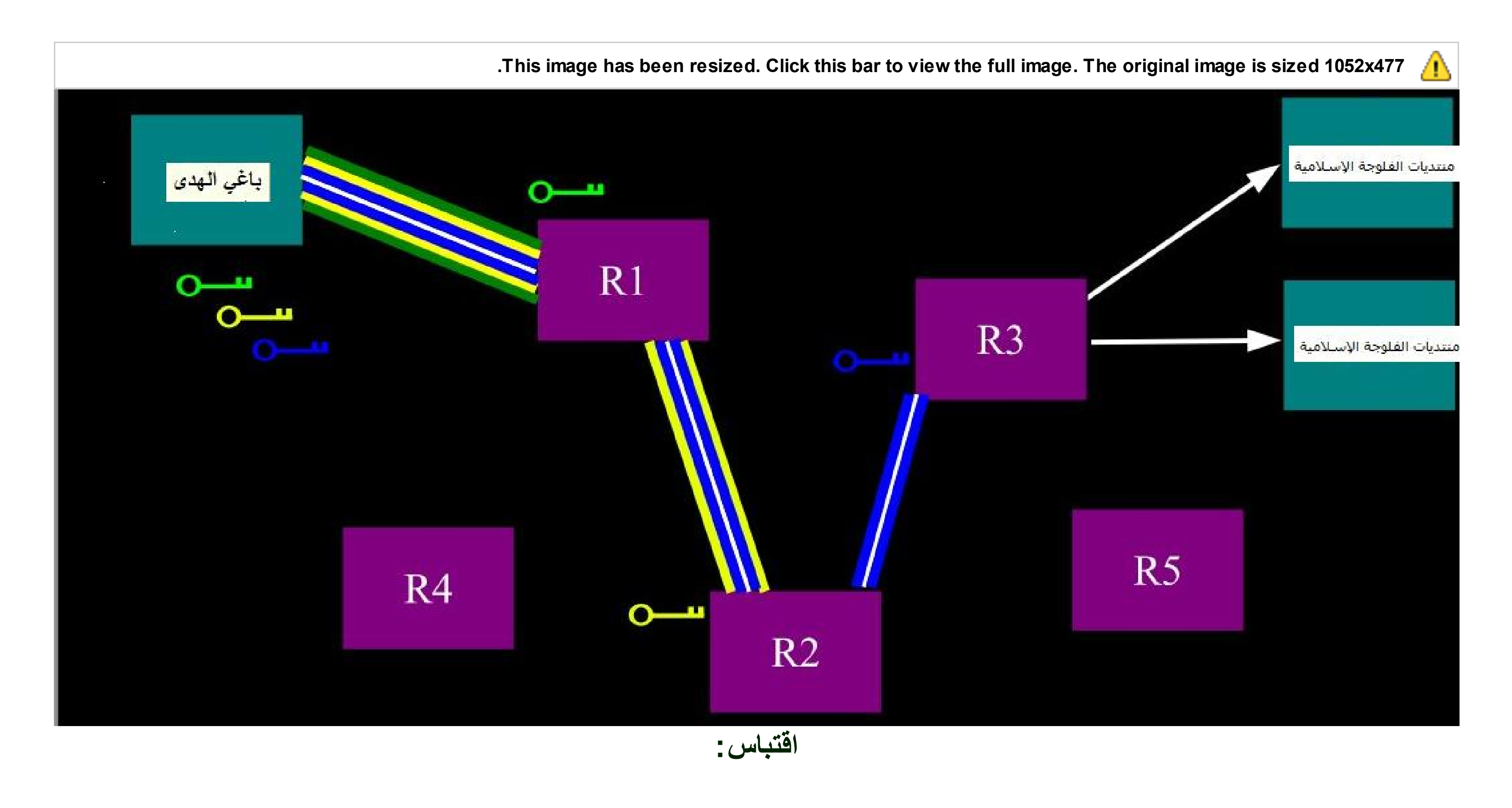
**فيقوم سرفر ال*Privoxy* بتشفيرها (يقوم *Privoxy* بمهام أخرى كحفظ المؤقت لل****ز و حبس الإعلانات ...)**

**و إخراجها من حاسوبك من المنفذ 9050 إلى مجموعة من رواتر التور المنتشرة في العالم**



حيث يقوم كل روتر بحل جزء من التشفير بالمفتاح المخصص له

.This image has been resized. Click this bar to view the full image. The original image is sized 1052x477




اقتباس:

بالصورة أعلاه لاحظ وجود خطينأخضرين و أزرقين و أصفرين لأن هناك إرسال و استقبال

فالباكيت تخرج مشفرة ثلاث مرات و يتم حل التشفير تدريجيا ... و تعود غير مشفرة و يتمم التشفير تدريجيا ...فجهازك في نهاية الأمر يقستبل الباكيت ( أي باكيت
وTCP/IP الذي يتكون منه باكيتHTTP )مشفرا ثلاث مرات و يرسل الباكيت مشفر ثلاث مرات

(بروتوكول TCP/IP لا علاقة له مع رقم IP و أسشرح هذا الأمر لاحقا )

**إلى أن تصل إلى الروتر الأخير ( المسمى *Exit Node* ) هذا الأخير يقوم بإرسالها بالواضح إلى ال*Destination* ( سرفر الشركة المستضيفة للمنتدى )**

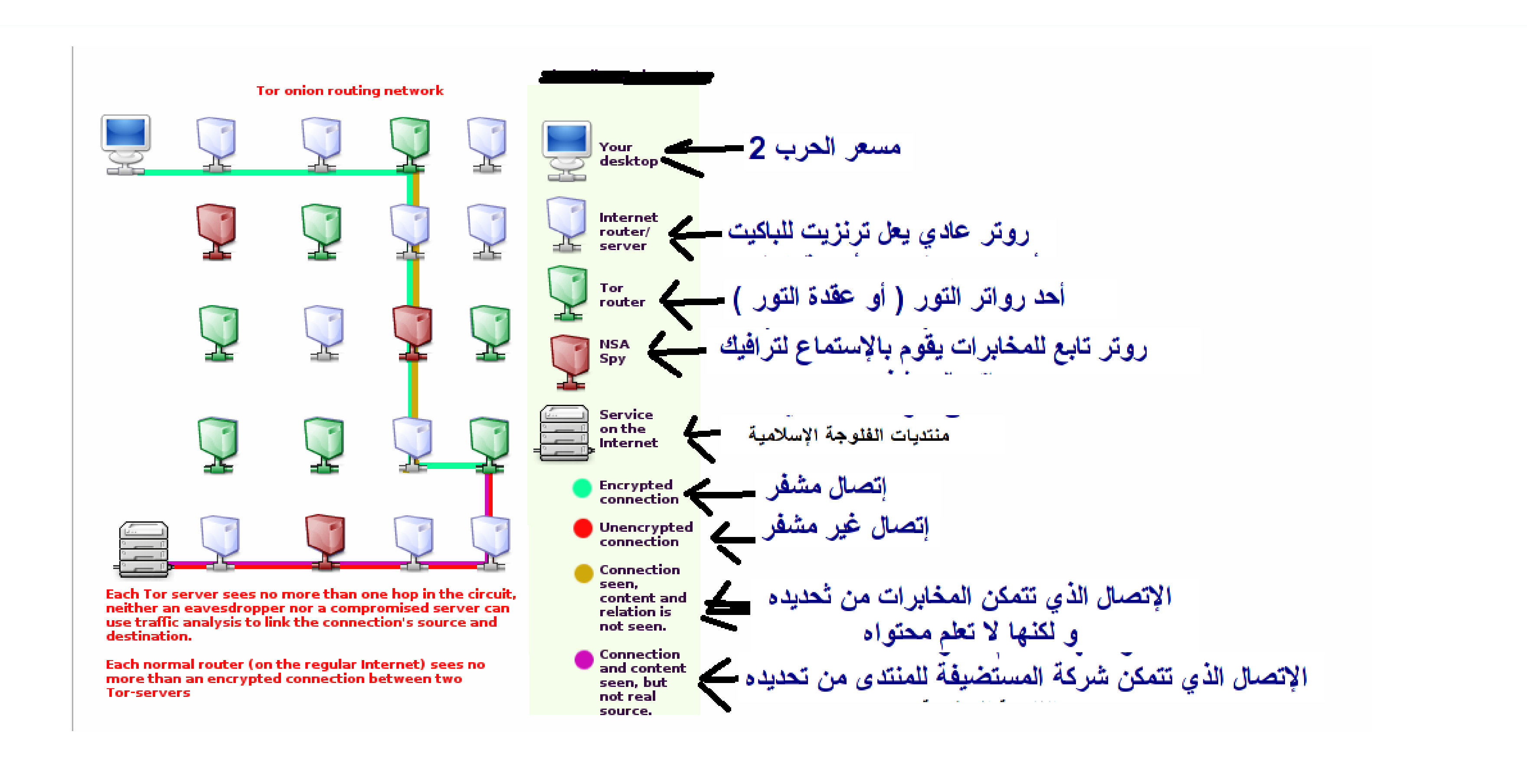
**( إذا كان المنتدى يدعم تقنية التشفيرSSL أي بروتوكول Https فإن الروتر الأخير يرسلها مشفرة )**

**بهذه الطريقة تضمن عدم إمكانية إلتقاط الباكيت من من طرف فلترات filters مخابرات بلادك المركبة على رواتر الترنزيـت المنتشرة في العالم**

**( مثلا عند إضافت رد في المنتدى يحتوي كلمة " جهــاد " لن يستطيع فلتر إلتقاط الباكيت الذي خصص للتقاط باكيت يحتوي على كلمة " جهــاد " لأنـها ستكون بكل بساطة مشفر كما يوضح هذا الرسم )**

**رسم يوضح *TCP/IP connection* بين مسعر الحرب2 و متندى الفـلوجة**

.This image has been resized. Click this bar to view the full image. The original image is sized 1015x535




بعد التدقيق في الصورة أعلاه ( دقيقتين على الأقل ) تستنتج أنه لا يمكن للمخابرات أن تحصل على أية معلومة عن مكان تواجدك و كل مايمكن أن تحصل عليه هو كلمة السر مسعر الحرب2 و لاشئ غير ذلك ( لأنه كما توضح الصورة الإتصال لايكون مشفر بين العقدة الأخيرة و المنتدى) و حتى لو ظلت تستعمل نفس Circuit لمدة طويلة ...

## ملاحظة

كما ذكرت سابقا كل عقدة تور تعلم العقدة التي يأتي منها الترافيك و العقدة التي عليها أن ترسل لها الباكيت

**حسنـــا الآن قد دققنا جيدا في الصور ( لا تنسى أن تدقق جيدا في الصور التي وضعتها )**

**و استطعنا و لله الحمد من فهم طريقة عمل التور**

**|**

**|**

**|**

**|**

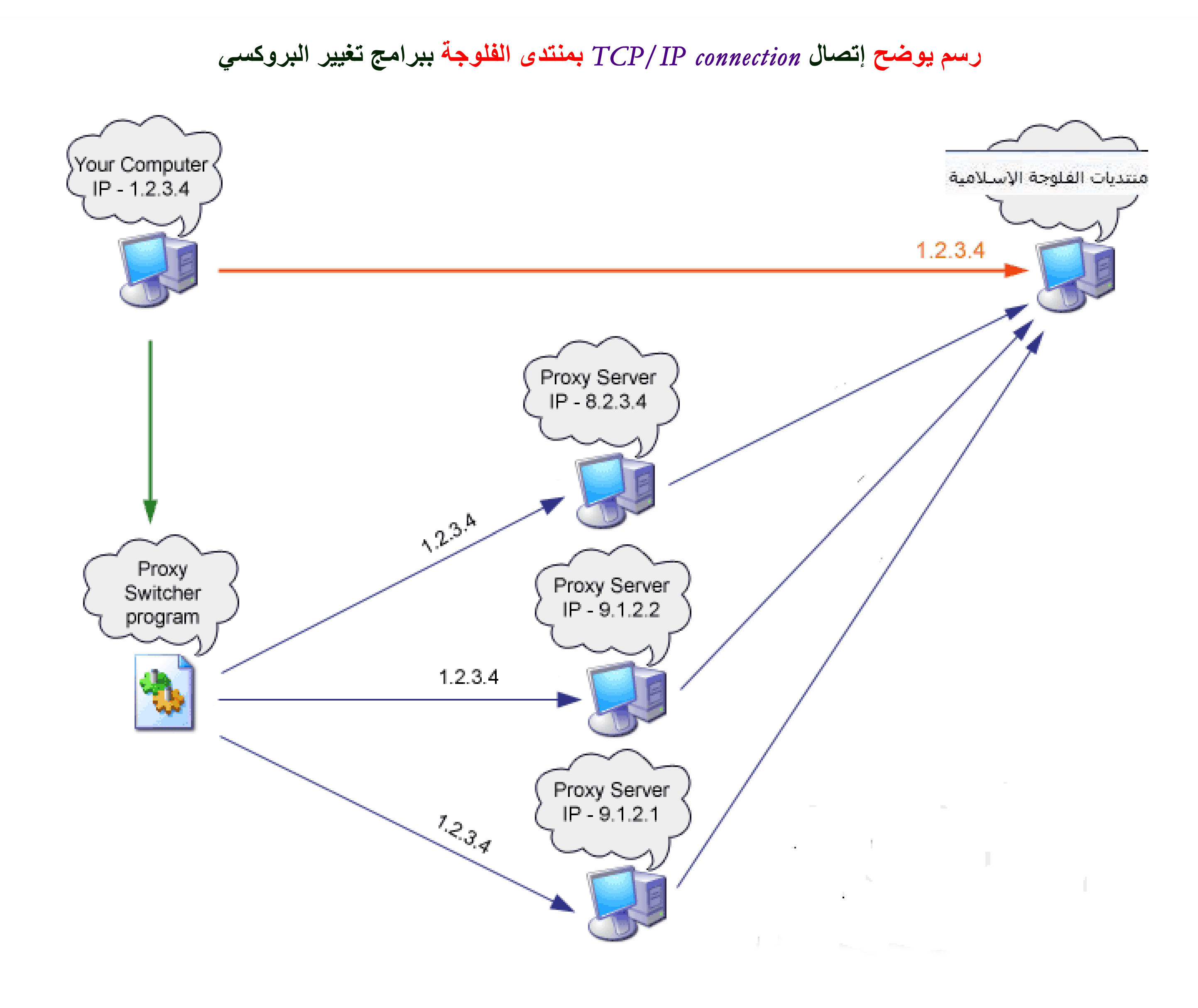
**|**

**V**

**كيفية يمكن لمخابرات البلاد التي تقطنها من التعرف على هويتك**

**الآن سنشرح كيف يمكن لمخابرات البلاد التي تقطنها من التعرف على هويتكبسهولة فائقة إذا كنت تستعمل برام تغيير البروكسي**

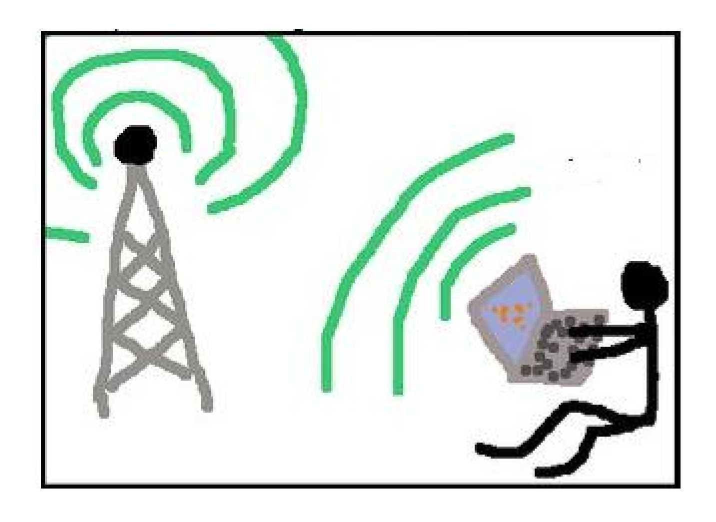
رسم يوضح إتصال *TCP/IP connection* بمنتدى الفلوجة ببرامج تغيير البروكسي




**يمكن لمخابرات البلاد التي تقطنها من التعرف على هويتك Online و ذلك من خلال**

# 1

**"الإستماع للترافيك ( *Traffic Sniffing* ) "**



**إلتقاط جميع ما يخرج من جهازيك ( مثلا مشاركة لك في المنتدى ) عن طريق فلترات مركبة على رواتر ( تم عام 2007 إعتقال مجموعة من الجهادين في ألمانيا عن طريق فلترات مراقبة الترافيك ) و اظنك تعلم بخبر اعتقالهم لأن الخبر أذيع على صعيد واسع في وسائل الإعلام )**

**اقتباس:**

**المخابرات تعمل traffic sniffing لعقد تبادل المعلومات على الإنترنت**

**مثلا بألمانيا هناك حوالي 120 عقدة تبادل traffic أكبرها عقدة التبادل الموجودة بمدينة Frankfurt و التي يمر منها حوالي 85% من Traffic المتوجه من ألمانيا إلى الخارج طبعا كما تعلمون برنامج التور Torيعمل Encryption لtraffic أي أنه لايمكن استناج أي شئ من عملية Sniffing إلا في حالة واحدة وهي إذا كان مخرج الحلقة أحد العقد التي تتجسس عليها الBND لأن المخرج لا يكون مشفرا ...و لكن حتى في هذه الحالة لا يمكن معرفة الإيبي ...**

**(ملاحظة لا يتم التقاط الباكت المار عن طريق شبكة التور لأنه يكون مشفر و غير مفهوم للفلتر )**

**أو**

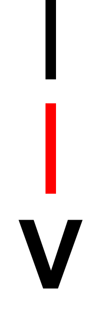
# 2

**من خلال طلب ملفات Logs البروكسي الذي استعمله برنامج تغيير البروكسي**
**( ملاحظة لا يتم الإحتفاظ بملفات على عقد التور )**
**أو**

# 3

**أن يكون البروكسي الذي يستعمله برنامج تغيير البروكسي تابع للمخابرات و هذا يسهل الأمور كثيرا على المخابرات فبرامج تغيير البروكسي تجلب البروكسيات التي تستعملها عن طريق عملية مسح لمواقع تجديد البروكسي فأي شخص يستطيع جعل حاسوبه بروكسي و يركب على حاسوبه أحد برامج الإستماع لترافيك مثل Wireshark ثم يضع رقم الإبي الخاص به على مواقع تجديد البروكسي فتقوم برامج تغيير البروكسي بجلب البروكسي (أي رقم الإبي و البورت ) ثم يتجسس على الباكيتات المارة**
**أو**
**etc.....**

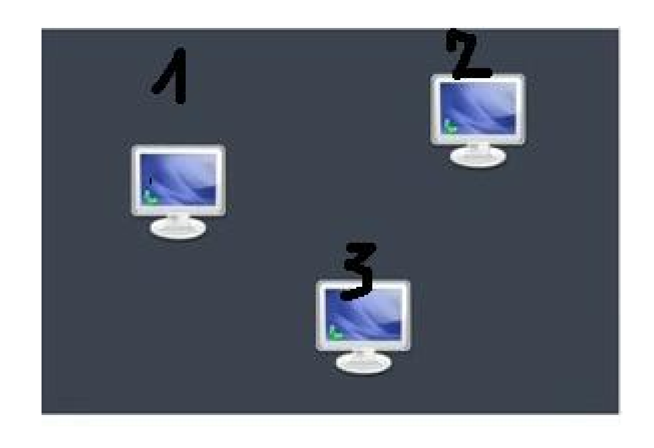
**حسنا و بعد أن قمت بقراءة هذه الفقرة ( عدة مرات مع التركيز ) استطعنا و لله الحمد فهم كيف يمكن لمخابرات البلاد التي تقطنها من التعرف على هويتك بسهولة فائقة إذا كنت تستعمل برام تغيير البروكسي**



**الآن سنشرح كيف يمكن اصطيادك كالسمكة و ذلك باستعمال سرفرات *DNS***

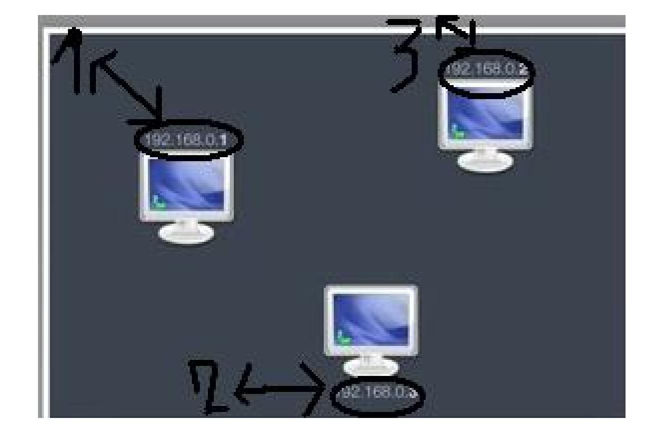
**سنضطرللرجوع إلى الوراء بحوالي 40 سنة ........**
**لأنني لا حظت أن بعض الإخوة ( إن لم أقل معظمهم ( لا يعلمون إلى حد الآن بعض الأشياء المهمة جدا التـي حدثت قبل 40 سنة**

**حسنا نحن الآن في سنة 1969**
**لدينا ثلاث أجهزة حاسوب نريد أن نشكل شبكة**



**المشكلة التي تواجهنا هي كالآتي :**
**عند ربط هذه الشبكة بأسلاك كيف يمكن للحاسوب 1 أن يتعرف عل الحاسوبين 2 و 3**

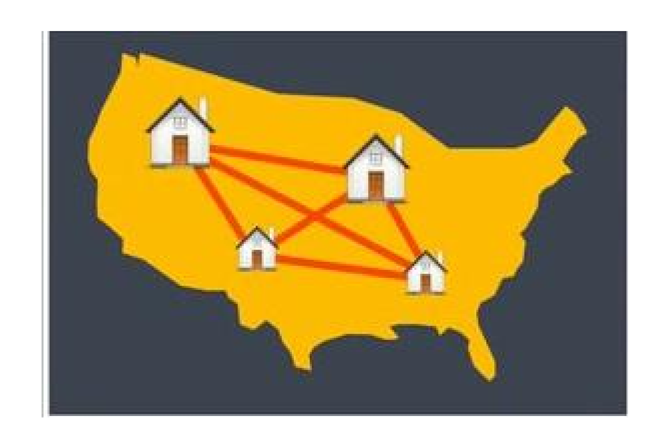
**تم التغلب على هذه المشكلة من خلال إعطاء أرقام لكل من الحواسب الثلاثة و هذه الأرقام هي ما يعرف ب Internet Protocol أي IP**



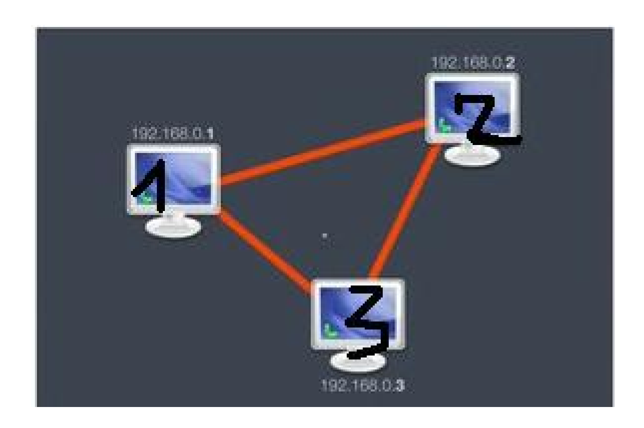

**نحن بني البشر نتعرف على بعضنا البعض من خلال أسمائنا فهناك شخص إسمه محمد و آخر إسمه علي و آخر إسمه حمزة ...و كل شخص يتعرف على بقية الأشخاص من خلال أسمائهم أما الحواسيب المرتبطة بشبكة فتتعرف على بقية الحواسيب الأخرى عن طريق أرقام IP**

**و هكذا في سنة 1969 قامت أربع جامعات أمريكية بالإرتباط مع بعضها البعض من خلال أسلاك و هكذا نشأت الإنترنت**

1969



**الآن لنرجع لمثالنا السابق لدينا ثلاث حواسيب مرتبطة فيما بينها**




**و سنقوم برفع منتدى الفلوجــة على الحاسوب1 رقم...**




## الحاسوب1يقدم الآن خِـدمَـة "تصفح المنتدى" للحاسوبين 2 و3

إذن إذا أراد الحاسوبين 2 أو 3 تصفح المنتدى فعليهم الإتصال بالحاسوب 1 ( رقم IP.... ) ليقوم بخدمَتهم و يوفر لهم إمكانية تصفح المنتدى

إذن فالحاسوب 1( رقم ) يلعب دور سرفر ( ف Server كلمة إنجليزية ترجمتها بالعربية هي خـادم ) لأنه يخدم الزبونين 2 و 3
أما الحاسوبين 2 و 3 فيلعباندور Clients ( ف Client كلمة إنجليزية ترجمتها بالعربية هي زبون ) لأنهم زبونين لدى الحاسوب 1 الذي يقوم بخدمتهما و ذلك لأنه يوفر لهما إمكانية تصفح المنتدى

إذا أراد الحاسوب 2 أو 3 تصفح المنتدى فعليهم أن يطلبو ذلك من الخـادم ( server ) أي الحاسوب1 الذي رفع عليه المنتدى و هذا الطلب يكون من خلال طلب رقم الإيبـي الخاص بهذا السرفر ( لا تنسى كلمة سرفر تعني خادم ) فنعد طلب هذا الرقم 202.75.39.82 نتصل بمنتدى الفلوجة و تظهر لنا صفحة المنتدى




1984

**حسنا الآن نحن في سنة 1984 و عدد الحواسيب المتصلة بالإنترنت أصبح كثير و كل حاسوب متصل بالشبكة لديه رقم IP خاص به و إذا أراد حاسوب الإتصال بحاسوب آخر فعليه طلب رقم IP الخاص بالحاسوب الذي يريد الإتصال به ...**
**حيث كل شخص لديه مجلدات يكتب فيها أرقام الإيبيات الكثيرة... و قد اختلطت الأمور كثيرا علينا الآن ...**

**لأننا بني البشر يصعب علينا تسجيل أرقام في ذاكرتنا بينما يمكن لنا تجيل أسماء بسهولة...**

# الحل

**و لحل هذه المشكلة سنقوم بتأسيس ما يســمى بسرفـرات DNS**

# فما هي سرفـرات DNS ؟
# و ما هو دورهــا ؟
# و ما هي طريقة عملها ؟

**D.N.S هي كلمة إنجليزية تعنـي Domaine Name Server**

**و سرفرات DNS هي حـــواسيب منتشرة في العالم تقدم الخدمة التالية :**

**تقوم سرفرات DNS بإعطــاء إسم بالأحرف اللاتنـة لكل رقم إيبي**
**فمثلا عوض كتابة الرقم 202.75.39.82 للإتصال بمنتدى الفلوجة يكفي أن نكتب faloja1.net فيقوم حاسوبنا بإرسال رسالة إلى سرفرات DNS يقول فيها ماهو رقم IP السرفر الذي رفع عليه الموقع التالي :**
**faloja.net**
**فتقوم سرفرات DNS بالتشاور مع بعضهـا البعض حتى تعثر على سرفر DNS يملك إجابة على هذا السؤال فيقوم سرفر DNS هذا, بإرسال رسالة إلى حاسوبنا الشخصي و يقول في تلك الرسالة إذا أردت الإتصال بموقع faloja1.net فعليك الإتصال بالحاسوب رقم 202.75.39.82 ( لا تنسى كلمة سرفر Server تعنى حاسوب يقدم خدمة )**

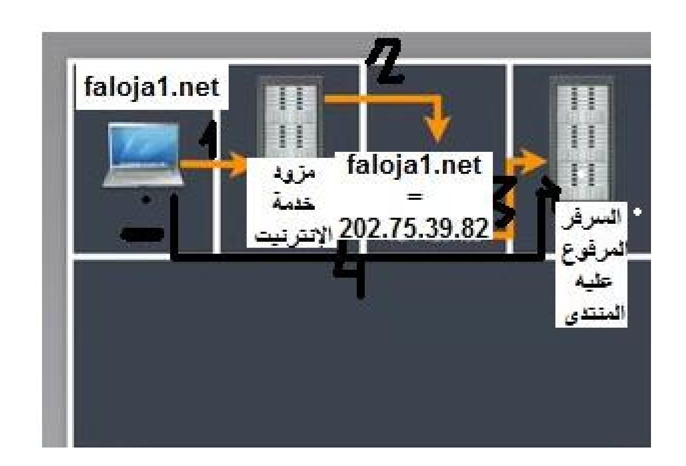
**و سرفرات DNS هذه منتشرة في العالم فهناك سرفر DNS خاص بمزود الخدمة في بلدك و هناك**
**سرفرات DNS خاصة ب ( com )**
**و أخرى خاصة ب ( info )**
**و أخرى خاصة ب ( org )**
**و أخرى خاصة ب ( net )**
**و أخرى خاصة بالبلدان مثلا السعودية لديها سرفرات خاصة بالمواقع ( sa)**
**و ألمانيا ( de )**
**و بريطانيا ( uk )**
**و ... و ...و ...**
**و هذه السرفرات مرتبة بشكل هرمي**
**بحيث حاسوبك عند طلب موقع ينتهي ب net**
**e.g:**
**faloja1.net**
**يقوم أولا بطلب رقم الإيبي من**
**سرفر DNS مزود الخدمة لديك ( في بلدك ) إذا لم يعثر عليه يقوم سرفر DNS مزود الخدمة لديك بطلب رقم الإيبيfaloja1.net من**
**سرفر DNS الخاص ب sa ( مثلا السعودية ) إذا لم يعثر عليه يقوم سرفرDNS ( الخاص ب sa ) بطلب رقم الإيبي من**
**سرفرDNS الأعلى في رأس الهرم عندها يقوم سرفرDNS الأعلى في رأس الهرم بطلب رقم الإيبي من**

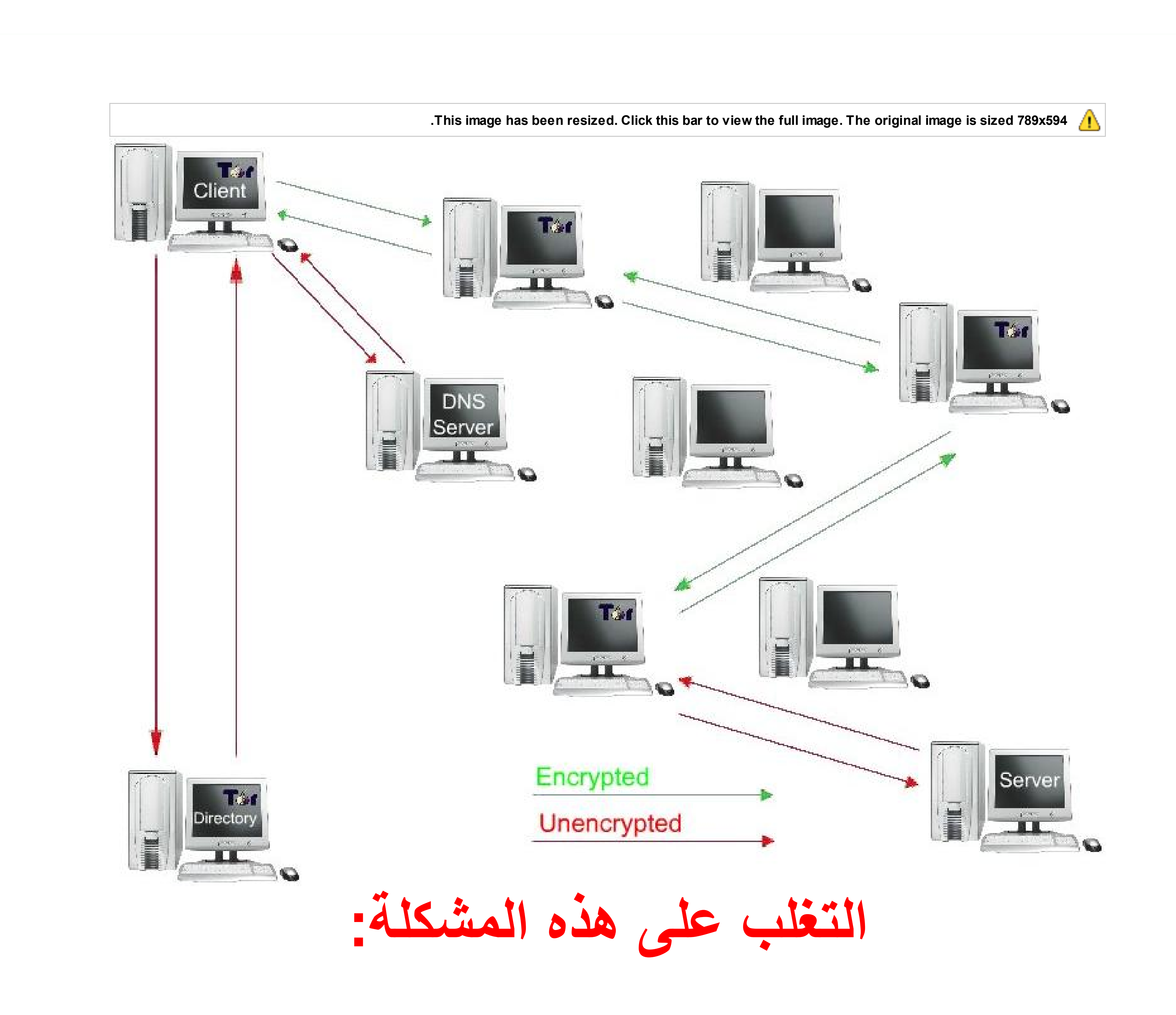
**سرفرات DNS المتفرعة عنه ..**
**فيجيبه سرفر DNS الخاص ب ( net )**
**أنا عندي رقم الإيبي الخاص بالموقع الذي طلبته**
**فيرسله لحاسوبك فيقوم حاسوبك بالإتصال بموقع**
**faloja1.net**
**عن طريق رقم الإيبي الذي حصل عليه ( 202.75.39.82 )**

**!!!**
**نعم نعم...!! لا تتعجب !!! كل هذا يحدث و أنث لا تشعر بشي ....لأن هذا يحدث بسرعة !**

## و هنا تدخل المخابرات في قصتنا .... كيف ذلك؟ ( إبتسامة ) ؟؟؟

**تطلب المخابرات من مزودي الخدمة بوضع السؤال ل faloja1.net في سرفرات DNS الخاصة بها لأن حاسوبك يسئلها قبل أن يسأل سرفرات DNS الأعلى منها فتعرف المخابرات أن رقم الإيبي الفلاني ( أي رقم الإيبي الخاص بك قد سأل عن رقم إيبي السرفر الذي يحتوي منتدى الفلوجة**
**ملاحظة:**
**( أن قلت أنها تعلم أنك اتصلت و لم أقل أنها تعرف أن معروفك في المنتدى هو... أو... فهذا لا يمكن معرفته إلا من خلال السرفر المرفوع عليه المنتدى و لكنها الآن تعلم أنك تتصل بالمنتدى و كم مرة اتصلت و هل تتصل كثيرا فتبدأ بالتجسس عليك )**






## التغلب على هذه المشكلة:

**ويمكن التغلب على هذه المشكلة بتمرير بيانات ال DNS في شبكة التور كما يوضح هذا الفديو**
**http://www.zshare.net/download/550193529c5ce90f/**
**أو للمشاهدة المباشرة**
**http://www.irongeek.com/i.php?page=videos/tor-1**

**أو**
**( و هذه هي الطريقة الأفضل )**
**الإتصال بالمنتدى عن طريق الرابط الرقمي :**

**http://202.75.39.82/~alfaloj/vb**

**فأنت باتصالك بالمنتدي ( يعني باتصالك بالسرفر الذي رفع عليه المنتدى)**
**( 202.75.39.82 )**
**لا تطلب أي شئ من سرفرات ال DNSلأنك تستعمل إسم الحاسوب الذي يقدم خــدمة المنتدى ليخــدُمَك مباشرة دون الحاجة لتمرير رسائل لسرفرات ال DNS**

# شرح الرابط :

*HTTP*
**يعنى بروتوكول إتصال إسمه http حيث تتصل عن طريق المنفذ رقم 80 في حـاسـوبك**

*202.75.39.82*
**يعني إسم الحاسوب الذي رفع علية المنتدى ( فأصبح ذالك الحاسوب بمثابة سـرفر أي خادم يقدم خدمة المنتدى )**

~

هذه العـــلامـة تعني أنظر تحت المجلد

*alfaloj/vb*

إسم المجلد الذي يجب النظر تحته

إذن أنت تتصل مباشرة بسرفر رقم *202.75.39.82* و تنظر تحت المجلد *alfaloj/vb* و هناك يوجد منتــدانـــا الغالــي

**مـلاحظة :**

**لمزيد من المعلومات حول كيفية عمل سرفرات DNS راجع**

**http://www.youtube.com/watch?v=k2oUZMKlozA**

اقتباس:

## كيف نعرف الرابط الرقمي لأي موقع نريده ؟

**سهلة جدا في أقل من ثواني كما موضح على الفديو**

**http://www.youtube.com/watch?v=Bva1QK_jl00**

**أو**

**ضع**

**Domain mane**

**أي**

**Website.com**

**بعد**

**/http://whois.domaintools.com**

**ليصبح**

**http://whois.domaintools.com/website.com**

**لمعرفة IP السرفر وwhois تعمل للموقع**

**أو**

**ركب هذا Add-on ل FireFox**

**https://addons.mozilla.org/en-US/firefox/addon/5791**

**Flagfox 3.3.7**

**و بعد التركيب سيظهر لك علم الدولة التي تحتوي على السرفر المركب عليه الموقع علي يمين خانت http Adress**
**إضغط زر يمـيـن على علم الدولة**

**و اختر whois و ستخرج لك كافة المعلومات عن الموقع**

## ملاحظة1

أحسن طريقة لتصفح الإنرتنت ::

1

إستعمـــال متصفح الفاير فوكس FireFox لتصفح المتندى بالتورTOR



2

إستعمـــال متصفح الأوبرى Opera لتتصفح في نفس الوقت الإنترنت بدون تور و بسرعة عالية



## ملاحظة2

كيفية معرفة الإتصالات المرتبطة بحاسوبك بدون أي برنامج فقط تكتب CMD للحصول على S H E L L ثم تكتب الأمر netstat للحصول على الإتصالات و هذا فديو :

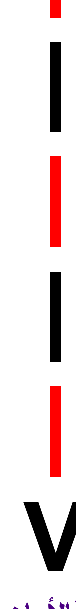
http://www.youtube.com/watch?v=RIKxI8HcdWI

يوضح كيفية استعمال الأمر netstat

طبق ما يوجد في الفديو!!!

هذا another فديو:

http://www.irongeek.com/i.php?page=v...-current-ports



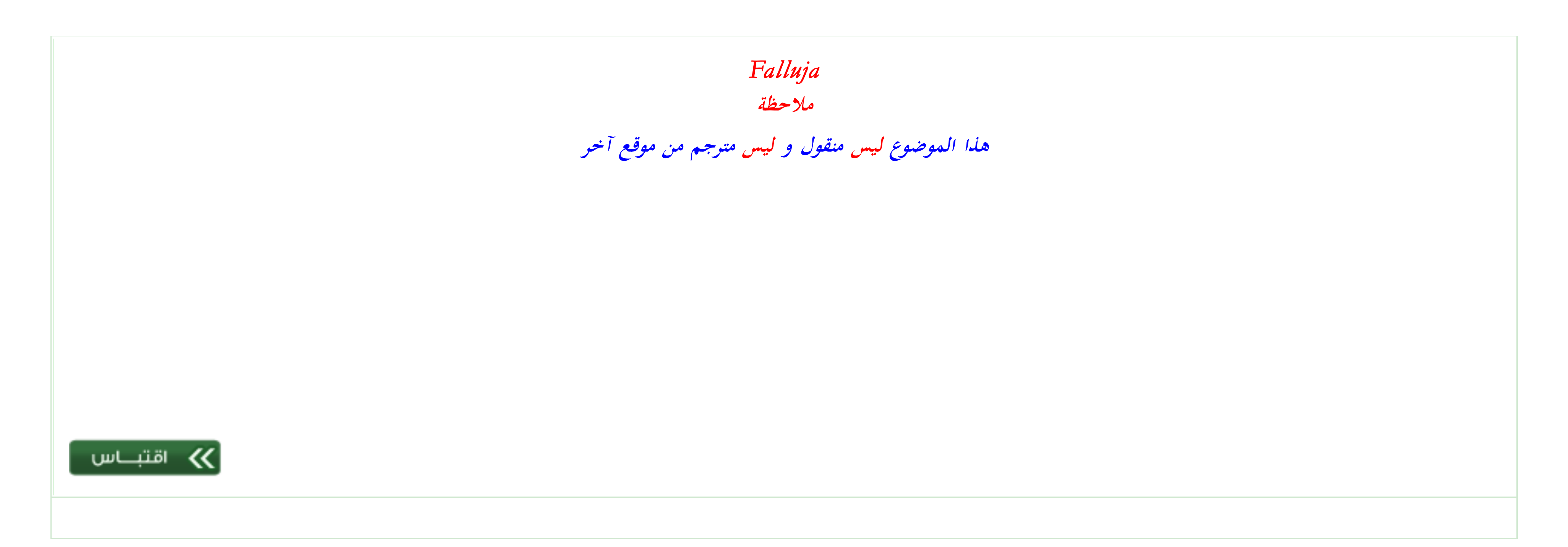
نحن لا نقول أننا سنخفي الإيبي و لكن سنصعب كثيرا إمكانية الحصول عليه ( فالأمان 100% غير ممكن ) و لكن علينا الأخذ بكافة الأسباب لأن الله أمرنا بذلك و علينا أن نجتهد في فهم كيفية عمل الأدواة و البرامج التي نستعملها و كذا طرق تطويرها و استعمالها بالطرق التي نريدهـا

يكفي أن نذكر أن:

الإنتربول الألماني بتعاون مع BND استولو على سرفرين لشبكة TOR أواخر 2006 لملاحقة شبكة دعارة للأطفال

**دون أي نتيجة...**

*Song of Terror*


Falluja
ملاحظة
هذا الموضوع ليس منقول و ليس مترجم من موقع آخر
اقتباس